学校编码：10384　　分类号_____密级_____
学号：X2010230659　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

基于 Web 的安全代码研究与应用

Research and Application of Secure Code Based on Web

施 炜

指 导 教 师： 林 坤 辉 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2012 年 10 月

论文答辩日期： 2012 年 11 月

学位授予日期： 年 月

答辩委员会主席：_____

评 阅 人：_____

2012 年 10 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

随着 Internet 重要性的不断增长，应用程序正呈高度互联的趋势。网站的安全性也面临巨大的挑战，传统的防火墙技术并不能很好的保证网站应用层的安全性。安全代码是从源码层面上减少系统漏洞、降低黑客攻击成功率，从而保证信息系统的安全性，完整性，可靠性和可用性的一种编码形式。因此，从安全代码角度解决网站的安全问题，能够减少网站的自身漏洞和加强网站的安全性。

Web 应用层存在许多的安全问题，如 SQL 注入，跨站点脚本攻击和跨站点请求伪造攻击。目前解决 Web 应用层安全的问题，大多通过购买高成本的硬件设备来抵御攻击，很少从代码层面考虑。在 Web 应用程序设计开发时，如果能从安全代码角度考虑安全问题，不仅解决了软件的安全性，也大大提高了应用程序自身的可靠性，而且降低了抵御入侵的成本。

本文首先论述了安全代码的研究背景、目的以及意义，其次介绍了安全代码相关技术，详细论述了 Web 应用层的安全漏洞和三种攻击方式。随后对 Web 安全代码模型进行了设计与实现，提供了各个模块的关键代码，并给出部署时的文件配置。最后，将安全代码模型运用到 Web 应用系统中，对比分析使用前后的结果，得出的结论符合本文的设计目标。

关键词：安全代码；安全代码模型；Web 应用层安全

Abstract

With the growing importance of the Internet, applications are becoming highly interconnected. The security of the website is also facing huge challenges and the traditional firewall technology can not guarantee the security of the website's application layer. The security code is a coded form that can reduce the number of application vulnerabilities and the rate of hackers' successful attacks, so as to ensure security, integrity, reliability and availability of the information systems. Therefore, writing security codes to solve the probleme of website security can not only reduce the vulnerabilities, but also strengthen the security of the website itself.

There are many security problems in the web application layer, such as sql injection, cross-site scripting attacks and cross-site request forgery attacks. At present, the solution to the security of the web application layer is mostly to purchase the high-cost hardwares while the security code is rarely considered to resist attacks. During the design and development of the web application, if the security code is taken into account, it will not only solve the security of the software and greatly improve the reliability of the application, but also reduce the cost of defense against intrusion.

The dissertation first describes the research background, purpose, and significance of the security code, followed by a brief introduction about the technology of the security code. Then it discusses in detail the security vulnerabilities of the web application layer and three ways of attacks. After that, it gives the design and implementation of the web security code model, providing the key codes for the various modules as well as the deployment configuration. Finally, the security code models are used into the web application systems. And through the comparative analysis of the results before and after the usage, it draws a conclusion which is in line with the design purpose of this dissertation .

Key Words: Secure Code； Secure Code Model； Web Application Security

目　录

第一章 绪 论 1

1.1 研究背景及意义 1

1.2 国内外研究状况概述 3

1.2.1 Web 安全研究状况 3
1.2.2 Web 安全代码研究状况 4

1.3 论文的主要内容和组织结构 5

第二章 代码安全相关技术 6

2.1 Web 站点理论 6

2.1.1 统一资源定位符 6
2.1.2 超文本传输协议 7
2.1.3 动态网页技术 8
2.1.4 网站的 Cookies 8
2.1.5 Web 的攻击分类 9

2.2 安全软件工程 9

2.2.1 定义安全性需求 10
2.2.2 安全性软件设计 10
2.2.3 安全编码 10
2.2.4 安全检测 11

2.3 密码及其它相关技术 11

2.4.1 对称密码和非对称密码技术 12
2.4.2 装饰器模式 13

2.4 本章小结 14

第三章 Web 应用层安全分析 15

3.1 Web 应用层安全漏洞 15

3.2 常见的几种攻击方式 17

3.2.1 SQL 注入攻击 17
3.2.2 跨站点脚本攻击 19
3.2.3 跨站点请求伪造攻击 21

3.3 造成的危害 24

3.3.1 SQL 注入攻击的危害 24
3.3.2 跨站点脚本攻击的危害 24
3.3.3 跨站点请求伪造攻击的危害 25

3.4 本章小结 25

第四章 Web 安全代码模型的设计与实现 26

4.1 模型设计原则 26

4.2 模型设计目标 26

4.3 模型的架构设计 27

4.3.1 模型的总体框架 27
4.3.2 模型的功能设计 29

4.4 模型的详细设计 35

4.4.1 过滤器的实现 35
4.4.2 安全会话模块的实现 37
4.4.3 安全日志模块的实现 39
4.4.4 各个模块整合的实现 40
4.5.2 文件配置 42
4.5.3 模型的部署 42

4.7 本章小结 43

第五章 Web 安全代码模型的应用 44

5.1 模型运用情况 44

5.1.1 原系统 APPSCAN 扫描结果 45
5.1.2 调用模型后系统扫描结果 46

5.2 对比分析 47

5.3 模型的特点分析 47

5.3.1 平台特性 47
5.3.2 功能特点 48

5.4 本章小结 48

第六章 总结与展望 49

6.1 总结 49

6.2 展望 49

参考文献 51

致谢 53

Contents

Chapter1 Introduction.....1

1.1 Background and Meaning of Dissertation.....1

1.2 Domestic And Foreign Reserch Profile.....3

1.2.1 Web Security Research Profile.....3

1.2.2 Web Secure Code Research Profile.....4

1.3 Content and Structure of Dissertation.....5

Chapter 2 Relevant Techniques of Secure Code.....6

2.1 Theory of Web Sites.....6

2.1.1 Uniform Resource Locator.....6

2.1.2 Hypertext Transfer Protocol.....7

2.1.3 Dynamic Web Technology.....8

2.1.4 Cookies of Web Sites.....8

2.1.5 Web Attack Classification.....9

2.2 Secure Software Engineering.....9

2.2.1 Define Security Requirement.....10

2.2.2 Security Software Design.....10

2.2.3 Secure Coding.....10

2.2.4 Security Test.....11

2.3 Cryptography And Other Related Technology.....11

2.4.1 Symmetric Password and Asymmetric Cipher Technology.....12

2.4.2 Decorator Pattern.....13

2.4 Summary.....14

Chapter3 Web Application Layer Security Analysis.....15

3.1 Web Application Layer Security Vulnerabilities.....15

3.2 Several Common Attacks.....17

3.2.1 SQL Injection Attack.....17

3.2.2 Cross Site Scripting Attack.....19

3.2.3 Cross Site Request Forgery Attack 21
3.3 The Attack's Damage 24
3.3.1 SQL Injection Attack Damage 24
3.3.2 Cross Site Scripting Attack Damage 24
3.3.3 Cross Site Request Forgery Attack Damage 25
3.4 Summary 25
Chapter4 Web Secure Code Model Design And Implementation 26
4.1 Design Principle of The Model 26
4.2 Design Objective of The Model 26
4.3 Model of Architecture Design 27
4.3.1 The Model General Framework 27
4.3.2 The Model Functional Design 29
4.4 Model of The Detailed Design 35
4.4.1 Filter Implementation 35
4.4.2 Secure Session Implementation 37
4.4.3 Secure Log Implementation 39
4.4.4 Module Integration Implementation 40
4.5.2 File Configuration 42
4.5.3 Model Deployment 42
4.7 Summary 43
Chapter5 Web Secure Code Model Application 44
5.1 The Model Application Situation 44
5.1.1 Original AppScan Scanning Results 45
5.1.2 Called The Model Scanning Results 46
5.2 Comparative Analysis 47
5.3 The Character of The Model Analysis 47
5.3.1 Speciality of Platform 47
5.3.2 Characteristic of Function 48
5.4 Summary 48
Chapter6 Conclusions and Future Work 49

6.1 Conclusions **49**

6.2 Future Work **49**

References **51**

Acknowledgements **53**